UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/589,891	06/09/2000	Scott Alexander Vanstone	6944.22	9015

27155 7590 06/16/2004

MCCARTHY TETRAULT LLP
SUITE 4900, P.O. BOX 48
66 WELLINGTON ST. WEST
TORONTO, ONTARIO, M5K 1E6
CANADA

EXAMINER	
HA, LEYNNA A	
ART UNIT	**PAPER NUMBER**
2135	13

DATE MAILED: 06/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/589,891	VANSTONE ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 April 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-50 have been re-examined. This is a FINAL rejection.

2. Claims 1-30 and 32-38 remains rejected under 35 U.S.C. 102(e).

3. Claims 31, 39, and 44-50 remains rejected under 35 U.S.C. 103(a).

4. Response to arguments.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

5. Claims 1-30 and 32-38 are rejected under 35 U.S.C. 102(e) as being anticipated by Vanstone, et al. (US 6,446,207).

As per claim 1:

Vanstone, et al. teaches a data transmission system including a plurality of correspondents interconnected by a data transmission link (col.2, lines 54-57) wherein the first correspondent is a smart card **12** and the second correspondent is a terminal in a banking institution **14**. Vanstone teaches the method of verifying a transaction between the first and second correspondents through the use of a certifying authority for verifying the validity of certificates (col.2, lines 2-12).

Vanstone discusses initiating a verification protocol by having one correspondents formulating a message (col.3, lines 23-24) and advising the certifying authority (CA) to validate the certificate wherein the CA (col.5, lines 57-60) generates signature components including authorization information (col.3, lines 30-45) and forwarding the signature component for permitting the first correspondent to generate a ephemeral or short term private key (col.3, lines 25-26). The second correspondent receives the signature component that permits the recovery of the short term public key corresponding to the short term private key (col.5, lines 6-15).

Vanstone further discloses the first correspondent signing a message with the short term private key (col.4, lines 38-43) and forwarding the message to the second correspondent where the second correspondent attempts to verify the signature using the short term public key and proceeds with the transaction upon verification (col.6, lines 28-35).

As per claim 2: Vanstone discusses initiating a verification protocol by the first correspondent formulating a message (col.3, lines 23-24).

As per claim 3: Vanstone discloses the second correspondent receives at least one of the signature components by the CA (col.5, lines 2-4).

As per claim 4: Vanstone discloses at least one of the signature components is forwarded to the first correspondent by the second correspondent (col.6, lines 17-20).

As per claim 5: See col.4, lines 40-43 and col.5, lines 25-65; discussing the signature components including long term private key and secure hash function and the long term private key of the first correspondent is sent to the CA prior to the verification transaction.

As per claim 6: See col.5, lines 57-60 and col.4, lines 40-43.

As per claim 7: See col.3, lines 50-53 and col.4, lines 57-60; discussing the identity of the first correspondent. The identity can be amongst many types of information such as the name, telephone number, and/or address and these distinguishing information uniquely identifies the destination associated to the secure transaction.

As per claim 8: As rejected on the same rationale as applied in claim 7.

As per claim 9: See col.3, lines 24-56 for short term private key.

As per claim 10: See col.5, lines 7-10 discussing short term public key and the CA's public key.

As per claim 11: See col.2, lines 11-12; discussing the CA authenticating or verifying its own certificates.

As per claim 12: See col.5, lines 7-10 discussing the private and public keys.

As per claim 13: Vanstone discusses initiating a verification protocol by the first correspondent formulating a message (col.3, lines 23-24).

As per claim 14: Vanstone discloses the second correspondent receives at least one of the signature components by the CA (col.5, lines 2-4).

As per claim 15: Vanstone discloses at least one of the signature components is forwarded to the first correspondent by the second correspondent (col.6, lines 17-20).

As per claim 16: See col.4, lines 40-43 and col.5, lines 25-65; discussing the signature components including long term private key and secure hash function and the long term private key of the first correspondent is sent to the CA prior to the verification transaction.

As per claim 17: See col.5, lines 57-60 and col.4, lines 40-43.

As per claim 18: See col.3, lines 50-53 and col.4, lines 57-60; discussing the identity of the first correspondent. The identity can amongst many types of information such as the name, telephone number, and/or address and these distinguishing information uniquely identifies the destination associated to the secure transaction.

As per claim 19: See col.3, lines 50-53 and col.4, lines 57-60; discussing the identity of the first correspondent. The identity can be amongst many types of

information such as the name, telephone number, date/time, and/or address and these distinguishing information uniquely identifies the destination associated to the secure transaction.

As per claim 20: See col.3, lines 24-56 for short term private key.

As per claim 21: See col.5, lines 7-10 discussing short term public key and the CA's public key.

As per claim 22: See col.2, lines 11-12; discussing the CA authenticating or verifying its own certificates.

As per claim 23: See col.5, lines 7-10 discussing the private and public keys.

As per claim 24: See col.3, lines 1-21; discussing the first and the second correspondents.

As per claim 25: See col.5, line 26 thru col.6, line 44; discussing the signature components wherein includes long term public key, large prime number, and secure hash.

As per claim 26: See col.5, lines 57-60 and col.4, lines 40-43.

As per claim 27: See col.3, lines 50-53 and col.4, lines 57-60; discussing the identity of the first correspondent. The identity can amongst many types of information such as the name, telephone number, and/or address and these distinguishing information uniquely identifies the destination associated to the secure transaction.

As per claim 28: See col.3, lines 50-53 and col.4, lines 57-60; discussing the identity of the first correspondent. The identity can be amongst many types of

information such as the name, telephone number, date/time, and/or address and these distinguishing information uniquely identifies the destination associated to the secure transaction.

As per claim 29: See col.3, lines 24-56 for short term private key.

As per claim 30: See col.5, lines 7-10 discussing short term public key and the CA's public key.

As per claim 32: See col.5, lines 7-10 discussing the private and public keys.

As per claim 33: See col.5, line 26 thru col.6, line 44; discussing the signature components wherein includes long term public key, large prime number, and secure hash.

As per claim 34: See col.5, lines 57-60 and col.4, lines 40-43.

As per claim 35: See col.3, lines 50-53 and col.4, lines 57-60; discussing the identity of the first correspondent. The identity can amongst many types of information such as the name, telephone number, and/or address and these distinguishing information uniquely identifies the destination associated to the secure transaction.

As per claim 36: See col.3, lines 50-53 and col.4, lines 57-60; discussing the identity of the first correspondent. The identity can be amongst many types of information such as the name, telephone number, date/time, and/or address and these distinguishing information uniquely identifies the destination associated to the secure transaction.

As per claim 37: See col.3, lines 24-56 for short term private key.

As per claim 38: See col.5, lines 7-10 discussing short term public key and the CA's public key.

As per claims 40-43: See col.6, lines 56-62 for predetermined period of validity.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 31, 39, and 44-50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone, et al. and further in view of Perlman, et al. (US 6,230,266).

As per claim 31:

Vanstone, et al. teaches a data transmission system including a plurality of correspondents interconnected by a data transmission link (col.2, lines 54-57) wherein the first correspondent is a smart card and the second correspondent is a terminal in a banking institution. Vanstone teaches the method of verifying a transaction between the first and second correspondents through the use of a certifying authority for verifying the validity of certificates

(col.2, lines 2-12). However, Vanstone fails to disclose the CA recertifies the certificate.

Perlman teaches an authentication method to efficiently and securely re-establish authentication system security after a detection of a compromise of one of the online-line revocation servers (OLRS) by recertifying the certificate without discontinuing the original certification and issuing new certificates (col.3, lines 22-53).

Therefore, it would have been obvious for the ordinary skilled in the art at the time of the invention to employ the teaching of Perlman within the system of, Vanstone, Et. Al., because by recertifying the principal's public keys reduces needless consumption of administrative overhead and without significantly reduce authentication system security (col.3, line 55 thru col.4, line 32).

As per claim 39: The same rationale of claim 31 applies.

As per claim 44:

Vanstone, et al. teaches a data transmission system including a plurality of correspondents interconnected by a data transmission link (col.2, lines 54-57) wherein the first correspondent is a smart card **12** and the second correspondent is a terminal in a banking institution **14**. Vanstone teaches the method of verifying a transaction between the first and second correspondents through the use of a certifying authority for verifying the validity of certificates (col.2, lines 2-12). Vanstone discusses initiating a verification protocol by

having one correspondents formulating a message (col.3, lines 23-24) and advising the certifying authority (CA) to validate the certificate wherein the CA (col.5, lines 57-60) generates signature components including authorization information (col.3, lines 30-45) and forwarding the signature component (col.3, lines 25-26). The second correspondent receives the signature component that permits the recovery public key for use in verifying the correspondent (col.5, lines 6-15). Vanstone further discloses forwarding the signature components from the CA to the correspondent to verify the signature (col.6, lines 28-35). However, Vanstone fails to disclose the CA recertifying the certificate.

Perlman teaches an authentication method to efficiently and securely re-establish authentication system security after a detection of a compromise of one of the online-line revocation servers (OLRS) by recertifying the certificate without discontinuing the original certification and issuing new certificates (col.3, lines 22-53 and col.9, lines 30-32).

Therefore, it would have been obvious for the ordinary skilled in the art at the time of the invention to employ the teaching of Perlman within the system of, Vanstone, Et. Al., because by recertifying the principal's public keys reduces needless consumption of administrative overhead and without significantly reducing authentication system security (col.3, line 55-64).

As per claim 45: See col.5, line 26 thru col.6, line 44; discussing the signature components wherein includes long term public key, large prime number, and secure hash.

As per claim 46: As rejected with same rationale applies in claim 44 and further Perlman teaches the signature components for the random number having changed value from the CA (col.7, lines 1-23).

As per claim 47:

Vanstone, et al. teaches a data transmission system including a plurality of correspondents interconnected by a data transmission link (col.2, lines 54-57) wherein the first correspondent is a smart card and the second correspondent is a terminal in a banking institution. Vanstone teaches the method of verifying a transaction between the first and second correspondents through the use of a certifying authority for verifying the validity of certificates (col.2, lines 2-12). However, Vanstone fails to disclose the values being changed for other certification periods.

Perlman discloses updating the time stamp and version information of the certification revocation (col.10, lines 13-35). Therefore, it would have been obvious for the ordinary skilled in the art at the time of the invention to employ the teaching of Perlman within the system of Vanstone because the values being changed for other certification periods determines whether there exist discrepancies to indicate compromise.

As per claim 48:

Vanstone discuss the signature components wherein includes long term public key, large prime number, and secure hash (col.5, line 26 thru col.6, line

44). However fails to However, Vanstone fails to disclose values of the certification period the values being changed for other certification periods.

Perlman discloses updating the time stamp and version information of the certification revocation (col.10, lines 13-35). Therefore, it would have been obvious for the ordinary skilled in the art at the time of the invention to employ the teaching of Perlman within the system of Vanstone because the values being changed for the certification periods determines whether there exist discrepancies to indicate compromise.

As per claim 49: See col.5, line 26 thru col.6, line 44.

As per claim 50:

Vanstone discuss the signature components wherein includes long term public key, large prime number, and secure hash (col.5, line 26 thru col.6, line 44). However fails to However, Vanstone fails to disclose values of the certification period the values being changed for other certification periods.

Perlman discloses updating the time stamp and version information of the certification revocation (col.10, lines 13-35). Therefore, it would have been obvious for the ordinary skilled in the art at the time of the invention to employ the teaching of Perlman within the system of Vanstone because it determines whether there exist discrepancies to indicate compromise.

Response to Arguments

7. Applicant's arguments filed April 8, 2004 have been fully considered but they are not persuasive.

Applicant argues that the prior art (Vanstone, Et Al.) fails to disclose a private-public key verification protocol. However, Vanstone discloses verifying the signature using the corresponding public key throughout the prior art (see COL.1, lines 30-40 COL.3, lines 10-13; COL.4, lines 35-43; and COL.5, lines 46-56). If the prior art seems to be discussing a private key verification protocol that both correspondents share a private key, it is merely showing the various protocols or alternative embodiments that exists for verification schemes. In addition to Vanstone teaching the use of a public key to verify the signature, the prior art also discloses that it is known in the art there exists private-public key verification protocols.

8. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., *recertifying keys on* every transaction with a single CA) **are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).**

Perlman does teach recertifying keys (COL.3, lines 50-53 and COL.9, lines 30-32). Claim 44, broadly reads on a particular instant of certifying a

correspondent through a certifying authority and the authority recertifies the key. Applicant argues claim 44 teaches, "recertifying keys on every transaction with a single CA", which by far is not in the claimed language. The claim language is broad for nowhere does the claim language states "every transaction with a single CA", thus, does not require for Perlman to recertify keys on "every transaction" with just a "single CA".

Conclusion

9. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (703) 305-3853. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100